添付資料

【今月の呼びかけ】

「 スマートフォンを安全に使おう！ 」

IPA では 2011 年 2 月にスマートフォンのウイルスに関する呼びかけ※1 を発表しましたが、その後も新しいウイルスが次々と発見されており、利用者にとってウイルス感染の脅威はますます高まってきています。

また、ここ最近の IPA のウイルス届出の状況においても、スマートフォン（特に Android 端末）を狙ったウイルスが検出され始めています。

このような状況を考慮し、今回改めてスマートフォンをとりまくウイルス事情を解説するとともに、スマートフォンを安全に使うためにとるべき具体的な手段を紹介します。

※1　IPA-2011 年 2 月の呼びかけ「スマートフォンのウイルスに注意！」
http://www.ipa.go.jp/security/txt/2011/02outline.html

図 1-1：スマートフォンがウイルスに狙われつつあるイメージ図

（1）最近のスマートフォンのウイルス事情

表 1-1 はこれまで IPA に届出のあった、Android 端末を狙ったウイルスの一覧です。

表 1-1：IPA に届出のあった、Android 端末を狙ったウイルス

届出時期	名称	特徴
2011 年 3 月	AndroidOS/Lotoor（ロトール）[DroidDream]（ドロイドドリーム）	ウェブサイトからダウンロードすることにより感染し、Android 端末に保存されている情報を収集、外部に送信するといった機能を有する。
2011 年 6 月	AndroidOS/Lightdd（ライトディーディー）	感染すると、Android 端末の情報を盗み取り、外部に送信する。
2011 年 6 月	AndroidOS/Smspacem（エスエムエスパーセム）	感染すると、Android 端末内のアドレス帳の連絡先に、SMS※2 メッセージの送信を試みる。
2011 年 6 月	AndroidOS/Smstibook（エスエムエスティブック）	感染すると、事前に設定された番号に、プレミアム SMS※3 メッセージの送信を試みる。

※2 SMS（Short Message Service）：携帯電話同士で、短い文章のメールを送受信できるサービス。
※3 プレミアム SMS：発信者がメッセージを送るだけで、相手先が利益を得る仕組みが付加された SMS。

このように、今年に入ってからスマートフォンを狙ったウイルスが次々と発見されており、利用者にとってウイルス感染の脅威がますます高まってきています。

また、スマートフォンがウイルスに感染してしまった場合に想定される被害例として、以下が考えら

れます。

- スマートフォン内データ、GPS※4による位置情報等、個人情報を含む重要な情報が悪意ある第三者に送られてしまう。
- 悪意ある第三者にスマートフォンを乗っ取られて、自由自在に操られてしまう。
- スマートフォンがボットネット※5の１つとして組み込まれ、知らぬ間に特定の組織にサイバー攻撃を行うなどの犯罪の道具として使われてしまう。

※4 GPS（Global Positioning System）：人工衛星の電波を使って、受信者の地球上の位置を割り出すシステムのこと。
※5 ボットネット：攻撃者が、ボットと呼ばれるウイルスに感染させた多くのコンピュータを使って、ターゲットに対し遠隔で攻撃を行うために構築されたネットワークのこと。

（2）IPA に届出のあったスマートフォンのウイルスについて

図 1-2 は 2011 年 3 月～2011 年 7 月に、IPA に届出のあったスマートフォンのウイルスの検出数のグラフです。

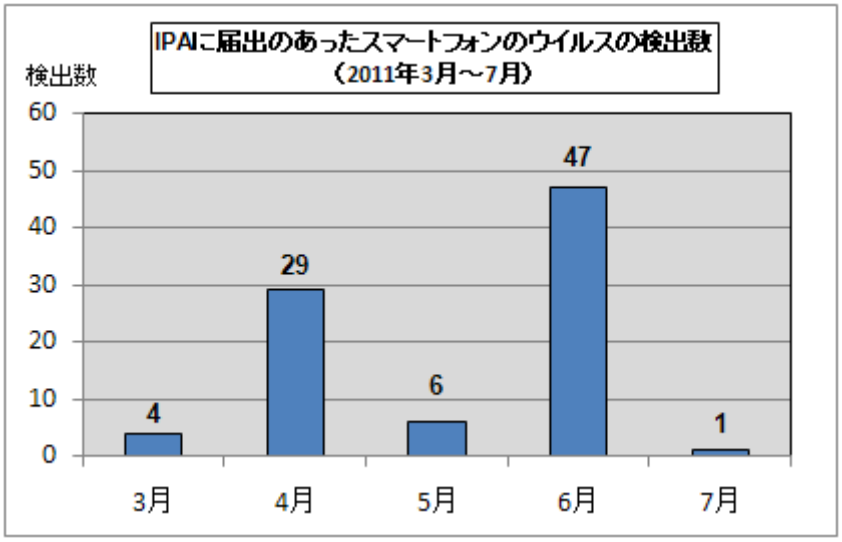

図 1-2：IPA に届けられたスマートフォンのウイルスの検出数（2011 年 1 月～7 月）

これらのウイルスは全て、スマートフォン上で発見されたものではなく、Windows などパソコンの環境でメール受信時などに検出されたものでした。メールにウイルスを添付して、それをスマートフォン上で開かせることでウイルス感染させようという意図から、メールが不特定多数に送られたため、パソコンにも届いているようです。加えて、Android 端末用のセキュリティソフトがあまり普及していないために、スマートフォン上でのウイルス発見の報告がまだないものと思われます。なお、2011 年 3 月から 7 月に届出のあったスマートフォンのウイルスは、全て Android 端末をターゲットとするものでした。

ウイルスが混入したアプリが添付されたメールをスマートフォンで受信した場合、スマートフォンの機種や OS によっても挙動が異なりますが、特に **Android 端末の場合はメール表示中の「インストール」ボタンを押すとアプリのインストールが開始され、ウイルスに感染してしまう場合がある**ため、取り扱いには十分注意する必要があります。図 1-3 は、Android アプリ（.apk ファイル）が添付されたメールをスマートフォン（端末名：GALAXY Tab/OS バージョン：Android 2.2）上で見た際の画面例です。

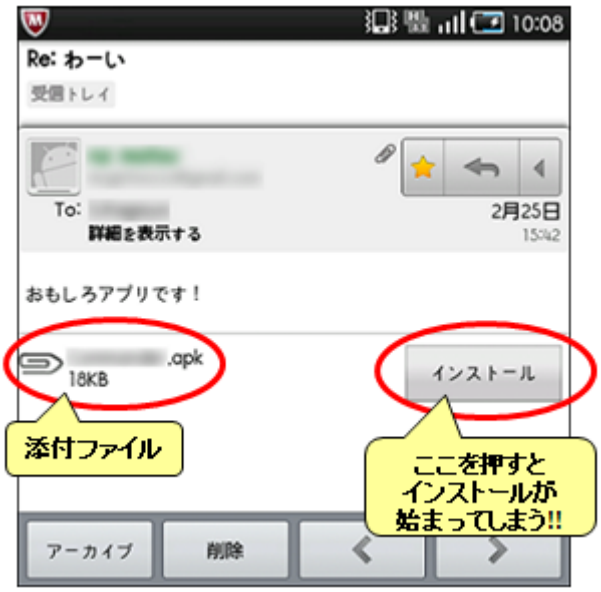

図 1-3：Android アプリが添付されたメールをスマートフォン上で見た画面例

（3）スマートフォンを安全に使用するための六箇条

上述したようなスマートフォンに関するウイルスの現状を受け、IPA では特にウイルスと脆弱（ぜいじゃく）性を悪用した攻撃への対策を考慮した、スマートフォンを安全に使用するための六箇条をまとめましたので、スマートフォン使用時の指針としてください（図 1-4 参照）。

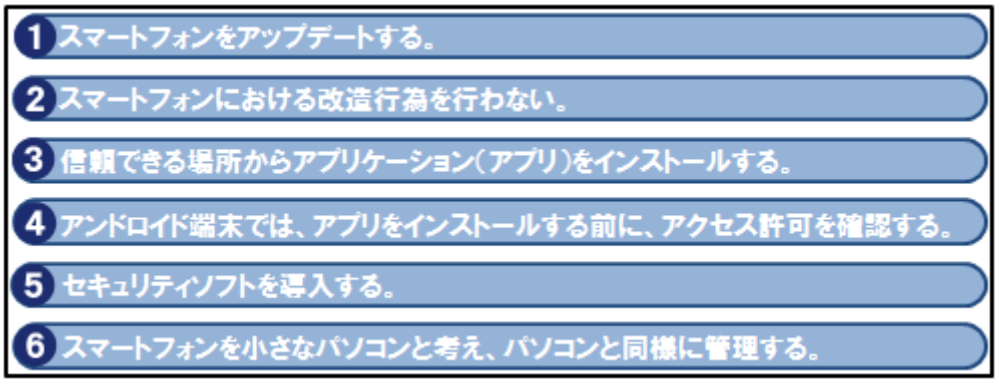

図 1-4：スマートフォンを安全に使用するための六箇条

各項目について以下に詳しく説明します。

【1】スマートフォンをアップデートする。

販売元から OS のアップデートが提供された場合、早めにアップデートしましょう。アップデートをしないで使っていると、パソコン同様、脆弱性を悪用した攻撃に遭う危険性が高まります。またその際、アップデート手順をきちんと理解することが重要です。アップデート手順は、販売元や製造元によって異なる場合があります。きちんとアップデートするために、取扱説明書などを確認し、正しい手順を身につけたうえでアップデートを実践しましょう。

【2】スマートフォンにおける改造行為を行わない。

スマートフォンにおける改造行為はやめましょう。ここでの改造行為とは、いわゆる iPhone における Jailbreak（脱獄）や Android 端末における root 権限奪取行為（root 化とも呼ばれる）などのことを指します。スマートフォンで動作するウイルスの中には、改造行為を行ったスマートフォンのみに感染するものも確認されています。ウイルス感染の危険性を自ら高めてしまうことになりますので、スマートフォンの改造行為はやめましょう。

【3】信頼できる場所からアプリケーション（アプリ）をインストールする。

スマートフォンで使用するアプリは、iPhone であれば米 Apple 社の「App Store」、Android 端末であればアプリの審査や不正アプリの排除を実施している場所（米 Google 社の「Android Market」）など信頼できる場所からインストールしましょう。

【4】Android 端末では、アプリをインストールする前に、アクセス許可を確認する。

Android 端末の場合、アプリをインストールする際に表示される「アクセス許可」（アプリが Android 端末のどの情報／機能にアクセスするか定義したもの）の一覧には必ず目を通しましょう（図 1-5 参照）。過去発見された Android 端末を狙ったウイルスには、個人情報などを不正に盗み取るため、アプリの種類から考えると不自然なアクセス許可をユーザーに求めるものがありました。例としては、壁紙アプリにも関わらず、アドレス帳の内容や通話履歴の記録へアクセスするための「連絡先データを読み取り」の許可を求めるなどといったものがあります。Android 端末にアプリをインストールする際に、不自然なアクセス許可や疑問に思うアクセス許可を求められた場合には、そのアプリのインストールを中止しましょう。

図 1-5：「アクセス許可」の表示画面の例

【5】セキュリティソフトを導入する。

スマートフォンの中でも Android 端末では、2011 年初頭以降大手ウイルス対策ソフトベンダーが続々とセキュリティソフトを発売し、その選択肢が充実してきました。Android 端末では**【4】**に注意すればウイルスに感染する可能性を低減できますが、ゼロにはできません。ウイルス感染の可能性をより低減するためにセキュリティソフトを導入してください。

【6】スマートフォンを小さなパソコンと考え、パソコンと同様に管理する。

企業でスマートフォンを活用する場合、スマートフォンの利用ルール、スマートフォンからアクセス可能な情報の範囲、スマートフォンに保存してよい情報の範囲、紛失・盗難時の対応等のポリシーを定めましょう。特に端末管理（MDM：Mobile Device Management）によって、スマートフォンに搭載されている OS のアップデートの徹底やインストールできるアプリの制限等を企業側が強制的に管理できる仕組みを設けることをおすすめします。